The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
10/13/2009

SUBJECT:
Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution (MS09-054)

OVERVIEW:
Four vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Microsoft Internet Explorer 5
- Microsoft Internet Explorer 6
- Microsoft Internet Explorer 7
- Microsoft Internet Explorer 8

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Four vulnerabilities have been discovered in Microsoft Internet Explorer. Details of these vulnerabilities are as follows:

Data Stream Header Corruption Vulnerability
A remote code execution vulnerability exists in the way Internet Explorer processes the data stream header. An attacker could exploit these vulnerabilities by constructing a specially crafted web page. When a user views the web page, the vulnerability could allow remote code execution.

HTML Component Handling Vulnerability
A remote code execution vulnerability exists in the way Internet Explorer handles validation of a variable. An attacker could exploit these vulnerabilities by constructing a specially crafted web page. When a user views the web page, the vulnerability could allow remote code execution.

Uninitialized Memory Corruption Vulnerability

Two remote code execution vulnerabilities exist in the way Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit these vulnerabilities by constructing a specially crafted web page. When a user views the web page, the vulnerability could allow remote code execution.

Successful exploitation could allow an attacker to execute arbitrary code on the affected system. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

While the vulnerability is in an IE component, there is an attack vector for Mozilla Firefox web browser. This occurs due to the .NET Framework 3.5 SP1 installing a Windows Presentation Foundation plug-in in Firefox. There is no patch for Mozilla Firefox.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- For Mozilla Firefox users with .NET Framework 3.5 installed, use “Tools”-> “Add-ons” -> “Plugins”, select “Windows Presentation Foundation”, and click “Disable”.

REFERENCES:

Microsoft:

http://www.microsoft.com/technet/security/Bulletin/ms09-054.mspx

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1547
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2529
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2530
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2531

Security Focus:

http://www.securityfocus.com/bid/36620
http://www.securityfocus.com/bid/36621
http://www.securityfocus.com/bid/36622
http://www.securityfocus.com/bid/36616